Termwork-4

Problem Statement

Using WIRESHARK observe the data transferred in client server communicating using UDP & identify the UDP datagram.

Objective

To observe the data transferred in client server communicating using UDP & identify the UDP datagram.

Theory

- Wireshark is a software tool used to monitor network traffic through a network interface
- Most widely used networking monitoring tool
- Users: system administrators, network engineers, black hat hackers.
- It has great GUI as well as convention CLI.
- It offers network monitoring on almost all types of network standards.
- It is free to use
- It was started by Gerald combes in 1997.

Basic features of wireshark

- Packet Monitor
  - This segment visually shows the packet flowing inside network

The packets are shown with following information

1. Source Address
2. Destination
3. Packet type
4. Hex dumps of Packets
5. Contents of packet in Text
6. Source Port
7. Destination Port.

Working with wireshark

- Import from capture file: This feature lets you import packets dump from a file to analyze further.
  + here are many formats supported by wireshark like .pcapng
- Export to capture file: Wireshark lets you save the results as a capture file to continue working on them at late point of time.
- Launch Wireshark: select an interface & click on fin icon to start capturing packets.
- save the results as capture file & exit after your done.

UDP Analysis using wireshark

Activity - Capture UDP traffic

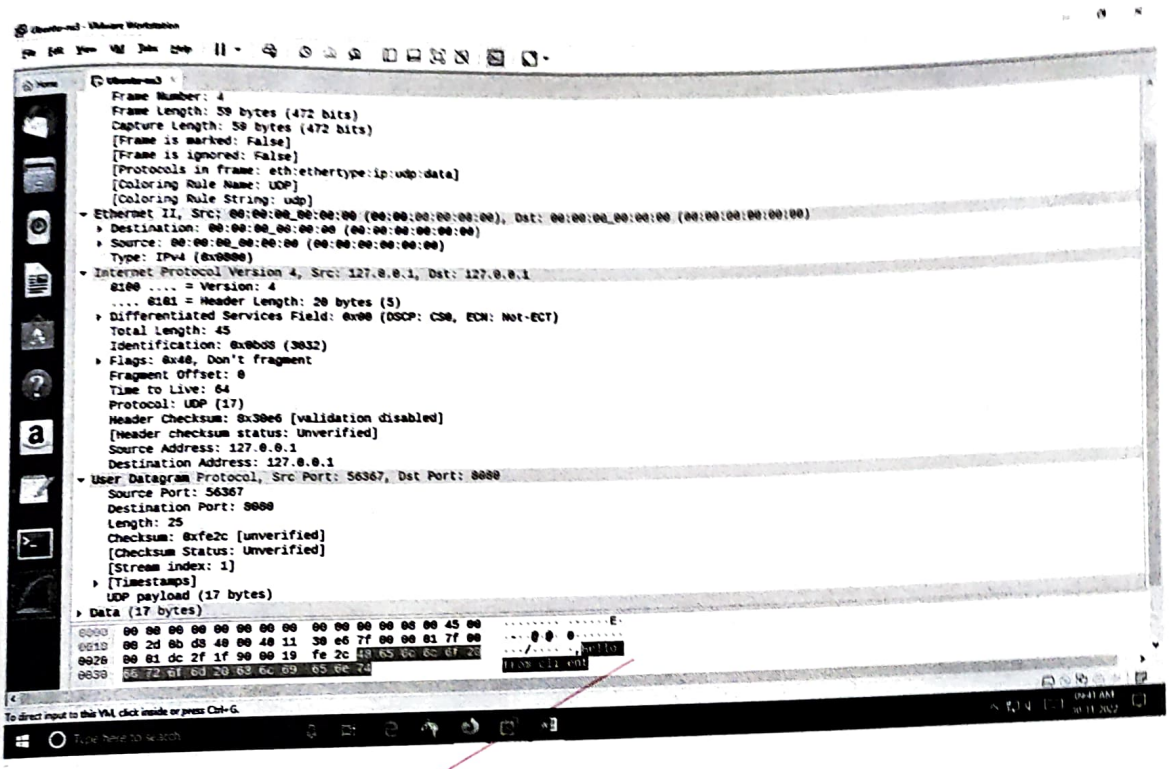
1. Start a wireshark capture
2. Open a command prompt
3. Type ipconfig /renew & press Enter to renew your DHCP assigned IP address. If you have a static address this will not generate any UDP traffic
4. Type ipconfig /flushdns & press Enter to clear your DNS name cache
5. Type nslookup 8.8.88 & press Enter to lookup the hostname for IP address 8.8.8.8
6. Close the command prompt
7. stop the wireshark capture.

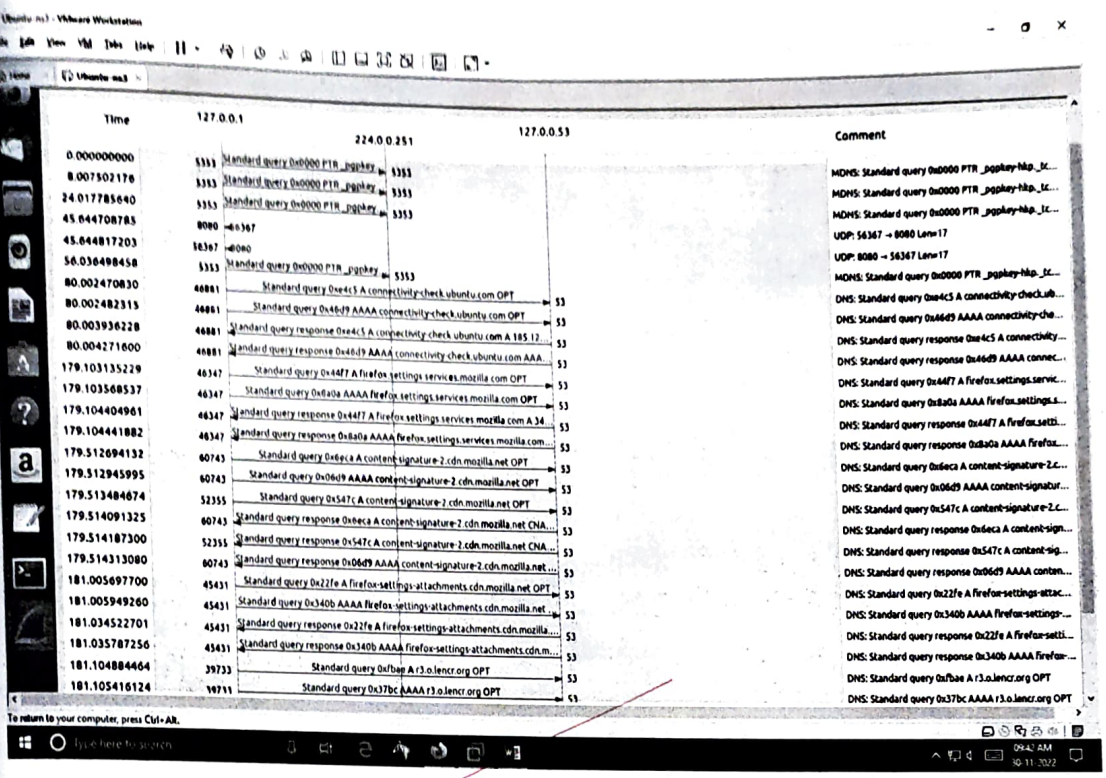
Term Work 4

Name:Vijay Anantpur

USN:2GI19CS176

Output:




Time
127.0.0.1
224.0.0.251
127.0.0.53
Comment
0.000000000 5353 Standard query 0x0000 PTR _pgpkey-hkp._tc... 5353 MDNS: Standard query 0x0000 PTR _pgpkey-hkp._tc...
8.007502176 5353 Standard query 0x0000 PTR _pgpkey-hkp._tc... 5353 MDNS: Standard query 0x0000 PTR _pgpkey-hkp._tc...
24.017785640 5353 Standard query 0x0000 PTR _pgpkey-hkp._tc... 5353 MDNS: Standard query 0x0000 PTR _pgpkey-hkp._tc...
45.044708785 8080 → 56367 UDP: 56367 → 8080 Len=17
45.044817203 56367 → 8080 UDP: 8080 → 56367 Len=17
56.036498458 5353 Standard query 0x0000 PTR _pgpkey-hkp._tc... 5353 MDNS: Standard query 0x0000 PTR _pgpkey-hkp._tc...
80.002470830 46881 Standard query 0xe4c5 A connectivity-check.ubuntu.com OPT 53 DNS: Standard query 0xe4c5 A connectivity-check.ub...
80.002482315 46881 Standard query 0x46d9 AAAA connectivity-check.ubuntu.com OPT 53 DNS: Standard query 0x46d9 AAAA connectivity-che...
80.003936228 46881 Standard query response 0xe4c5 A connectivity-check.ubuntu.com A 185.12... 53 DNS: Standard query response 0xe4c5 A connectivity-...
80.004271600 46881 Standard query response 0x46d9 AAAA connectivity-check.ubuntu.com AAA... 53 DNS: Standard query response 0x46d9 AAAA connec...
179.103135229 46347 Standard query 0x44f7 A firefox.settings.services.mozilla.com OPT 53 DNS: Standard query 0x44f7 A firefox.settings.servic...
179.103568537 46347 Standard query 0x8a0a AAAA firefox.settings.services.mozilla.com OPT 53 DNS: Standard query 0x8a0a AAAA firefox.settings.s...
179.104404961 46347 Standard query response 0x44f7 A firefox.settings.services.mozilla.com A 34... 53 DNS: Standard query response 0x44f7 A firefox.setti...
179.104441882 46347 Standard query response 0x8a0a AAAA firefox.settings.services.mozilla.com... 53 DNS: Standard query response 0x8a0a AAAA firefox....
179.512694132 60743 Standard query 0x6eca A content-signature-2.cdn.mozilla.net OPT 53 DNS: Standard query 0x6eca A content-signature-2.c...
179.512945995 60743 Standard query 0x06d9 AAAA content-signature-2.cdn.mozilla.net OPT 53 DNS: Standard query 0x06d9 AAAA content-signatur...
179.513484674 52355 Standard query 0x547c A content-signature-2.cdn.mozilla.net OPT 53 DNS: Standard query 0x547c A content-signature-2.c...
179.514091325 60743 Standard query response 0x6eca A content-signature-2.cdn.mozilla.net CNA... 53 DNS: Standard query response 0x6eca A content-sign...
179.514187300 52355 Standard query response 0x547c A content-signature-2.cdn.mozilla.net CNA... 53 DNS: Standard query response 0x547c A content-sig...
179.514313080 60743 Standard query response 0x06d9 AAAA content-signature-2.cdn.mozilla.net ... 53 DNS: Standard query response 0x06d9 AAAA conten...
181.005697700 45431 Standard query 0x22fe A firefox-settings-attachments.cdn.mozilla.net OPT 53 DNS: Standard query 0x22fe A firefox-settings-attac...
181.005949260 45431 Standard query 0x340b AAAA firefox-settings-attachments.cdn.mozilla.net ... 53 DNS: Standard query 0x340b AAAA firefox-settings-...
181.034522701 45431 Standard query response 0x22fe A firefox-settings-attachments.cdn.mozilla.... 53 DNS: Standard query response 0x22fe A firefox-setti...
181.035787256 45431 Standard query response 0x340b AAAA firefox-settings-attachments.cdn.m... 53 DNS: Standard query response 0x340b AAAA firefox-...
181.104884464 39733 Standard query 0xfbae A r3.o.lencr.org OPT 53 DNS: Standard query 0xfbae A r3.o.lencr.org OPT
181.105416124 39711 Standard query 0x37bc AAAA r3.o.lencr.org OPT 53 DNS: Standard query 0x37bc AAAA r3.o.lencr.org OPT
To return to your computer, press Ctrl+Alt.
Type here to search
09:42 AM
30-11-2022

30/11/22

Conclusion

We could observe the data transfered in client-server communicating using UDP & identify the UDP datagram using wireshark tool

Learning outcomes

- Understand the significance of Wireshark tool
- Understand how to analyze the UDP datagram using wireshark

References

- https://www.wireshark.org
- W Richard Stevens, Bill Fenner, Andrew M Rudoff: "UNIX Network Programming", Volume 1, Third Edition, Pearson 2004

2GI19CS176

Termwork-5

Problem statement

Using WIRESHARK analyse three way handshaking connection establishment, data transfer & connection termination in client-server communication using TCP

Objective:

To analyse three way handshaking connection establishmen data transfer & connection termination in client-server communication using TCP

Theory

Wireshark

- It is a software tool used to monitor the network traffic through a network interface
- Most widely used network monitoring tool
- Users: system administrators, network engineers, network enthusiasts, network security professionals
- It has great GUI as well as a conventional CLI
- It offer network monitoring on almost all types of network standards
- It is free to use
- It was started by Gerald Combez in 1997

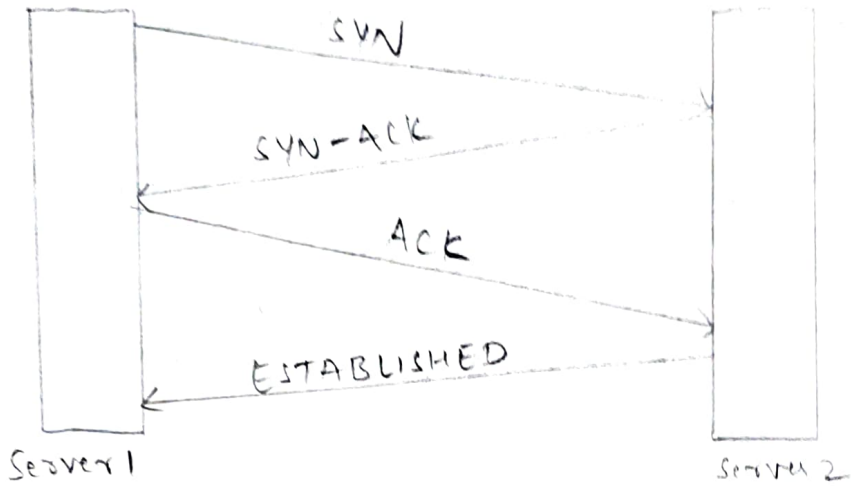
Basic features of wireshark

- Packet Monitor
  - This segment visually shows the packet flowing inside network

The packets all shown with following information

1. Source Address
2. Destination
3. Packet type
4. Hex dumps of Packets
5. Contents of packet in Text
6. Source port
7. Destination port.

Three way Handshake



Working with Wireshark

- Import from a capture file: This feature lets you import packets dump from a capture file to analyze further. There are many formats supported by wireshark like
  - .pcapng.
- Export to a capture file: Wireshark lets you save the results as a capture file to continue working on them at later point of time. The supported formats are .pcapng
- Launch wireshark, select an interface & click on fin icon to start capturing packets.
- Save the result as a capture file & exit after you are done seeing traffic.

TCP Analysis using Wireshark

- From menu bar, select capture → options → interfaces
- In the interfaces chose a particular interface, note down its IP, & click start button of selected adapter.
- This starts capturing packets.
- Run the TCP server & client programs to generate n/w
- Observe the packets ACK, SYN, SYN-ACK listed on their respective side.
- Source port:- This is port of host network used for communicat
- Destination port:- This the port of destination server.
- TCP segment length:- It represents data length in selected pact
- Sequence number:- It is a method used by wireshark to give particular indexing to each packet for tracking packets.
- Next sequence number:- It is sum of sequence number & the segment length of current packet.

Header length: It is length of TCP header & can vary from 20 to 60

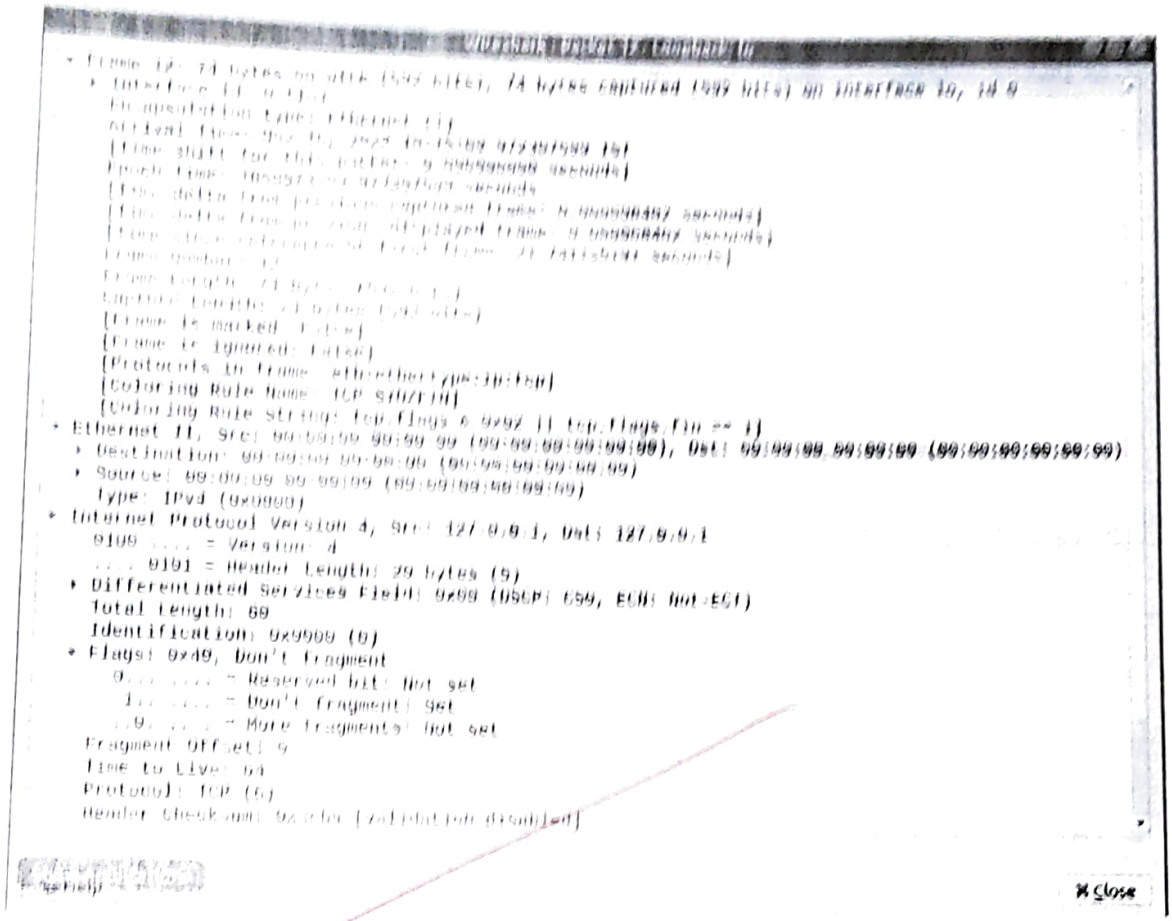
- A major section of this TCP packet analysis is flag section of packet which gives further in-depth information about packet
- The flag section has following parameters which are enlisted with their respective significance
- Congestion Window Reduced (CWR) - It signals a decrease in transmission rate.
- ECN-Echo : It is set on receiving router congestion notification
- Urgent : It is set when the packet is to be considered a priority.
- Acknowledgement : It indicates whether current packet contains an acknowledgement packet or not
- Push : The data should be saved & removed from channel
- Reset : It indicates an error in communication
- SYN : Packet is synchronized or not
- FIN : Finalization - end of communication, subsection
- Window size value : This is buffer size of current host
- checksum : It is used to verify that recieved packet is OK or has an error.
- checksum status :- The packet checksum is not verified by default but one can enable it as per requirements.

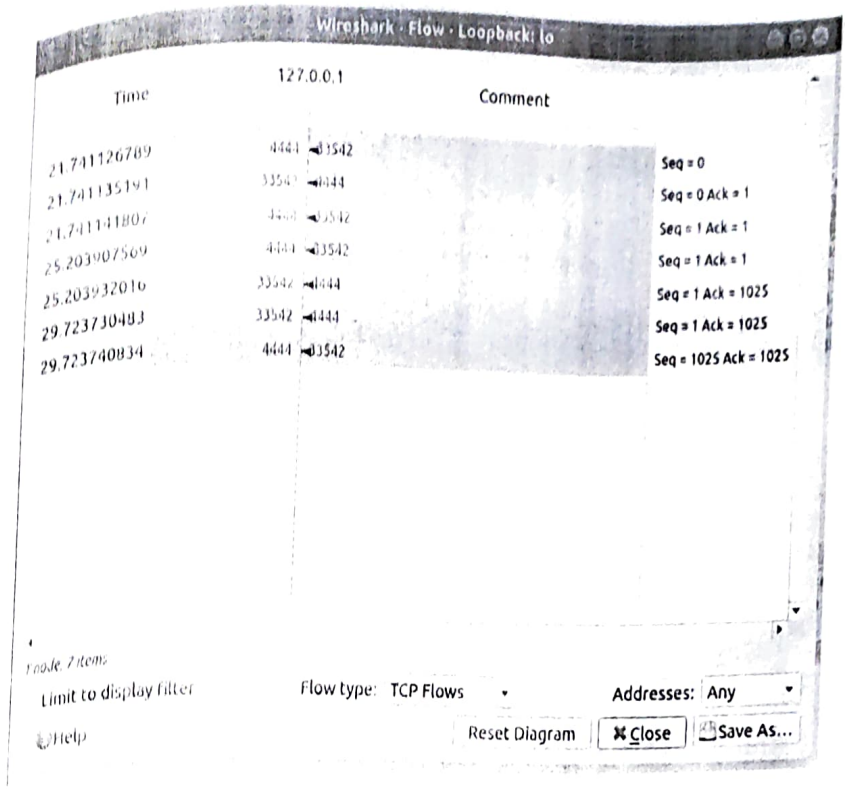
TermWork 5

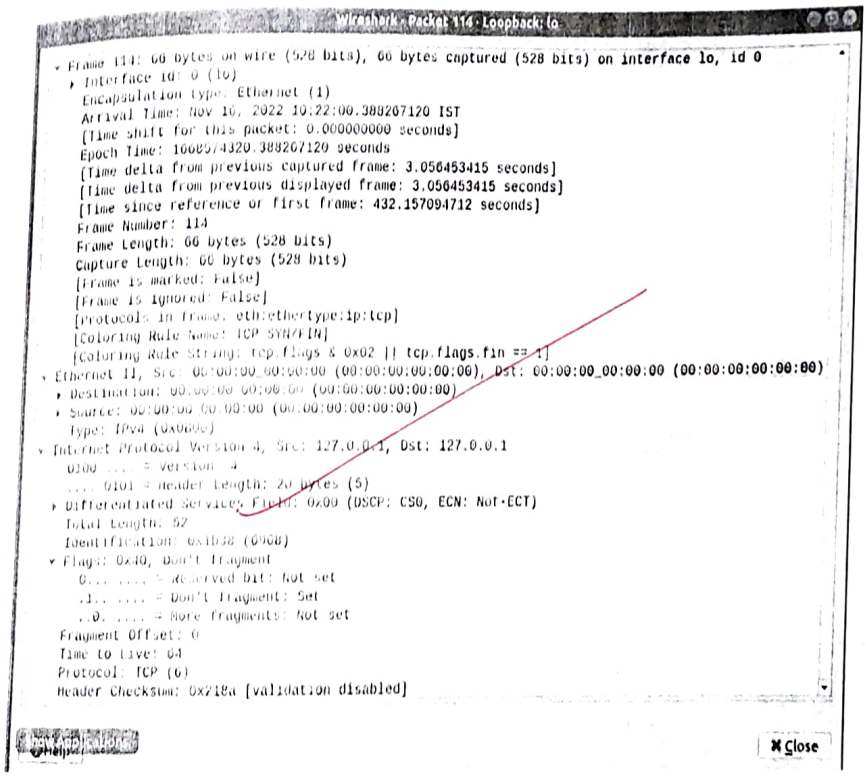
Name:Vijay Anantpur

USN:2GI19CS176

Output:




Wireshark · Flow · Loopback: lo
127.0.0.1
Time
Comment
21.741126789
21.741135191
21.741141807
25.203907569
25.203932010
29.723730483
29.723740834
4444 ⇄ 33542
33542 ⇄ 4444
4444 ⇄ 33542
33542 ⇄ 4444
4444 ⇄ 33542
Seq = 0
Seq = 0 Ack = 1
Seq = 1 Ack = 1
Seq = 1 Ack = 1025
Seq = 1 Ack = 1025
Seq = 1025 Ack = 1025
Limit to display filter
Flow type: TCP Flows
Addresses: Any
Help
Reset Diagram
Close
Save As...


Wireshark · Packet 114 · Loopback: lo
Frame 114: 60 bytes on wire (528 bits), 60 bytes captured (528 bits) on interface lo, id 0
Interface id: 0 (lo)
Encapsulation type: Ethernet (1)
Arrival Time: Nov 10, 2022 10:22:00.388207120 IST
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1668574320.388207120 seconds
[Time delta from previous captured frame: 3.056453415 seconds]
[Time delta from previous displayed frame: 3.056453415 seconds]
[Time since reference or first frame: 432.157094712 seconds]
Frame Number: 114
Frame Length: 60 bytes (528 bits)
Capture Length: 60 bytes (528 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp]
[Coloring Rule Name: TCP SYN/FIN]
[Coloring Rule String: tcp.flags & 0x02 || tcp.flags.fin == 1]
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Destination: 00:00:00_00:00:00 (00:00:00:00:00:00)
Source: 00:00:00_00:00:00 (00:00:00:00:00:00)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 52
Identification: 0x1b38 (6968)
Flags: 0x40, Don't Fragment
0... .... = Reserved bit: Not set
.1.. .... = Don't Fragment: Set
..0. .... = More fragments: Not set
Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x218a [validation disabled]
Close

10/10

30/11/22

Conclusion

We could analyze three way handshaking connection establishment data transfer & connection termination in client-server communication using TCP.

Learning outcomes

- Understand the significance of wireshark tool
- Understand how to analyze the TCP packets using Wireshark

References

https://www.wireshark.org

W. Richard Stevens, Bill Fenner, Andrew. M. Rodoff : "UNIX Network Programming", Volume 1, Third Edition Pearson 2004.